تعرف على الـ Brute Force

الـ BruteForce هي تقنية تخمين الأرقام السرية سواء بشكل يدوي او بأستخدام أداة .
ببساطة عملية محاولة اكتشاف الأرقام السرية من خلال تخمينها بقواميس مهيئة مسبقاً
تحتوى على ارقام / حروف / كلمات / ارقام سرية مستخدمة كثيراً .

أمثلة على أدوات تعمل على التخمين :

Cpanel Password Brute Force Tool
أداة مبرمجة بلغة Perl تعمل على تخمين password لوحة تحكم المواقع الشهيرة Cpanel .
الأداة تقوم بعملية التخمين من خلال قواميس من الارقام والحروف والرموز .
تعمل الأداة على مقارنة محتويات القاموس ان صحة التسمية مع لوحة تحكم التي تتم مهاجمتها .
وعند مطابقة احد محتويات القاموس مع الرقم السري للوحة يتم تخزينه بملف Text وعرضه للمستخدم .
و أداة THC-Hydra الرائدة بهذا المجال تعمل على تخمين كلمات المرور وتعمل على العديد
من البروتوكولات مثل http وتصل لأمكانية التخمين على البروتوكولات الأمنة التي تستخدم التشفير SSL .
وأيضا توجد العديد من الأدوات التي تعمل على التخمين لمختلف الخدمات
حتى أني رايت ذات مرة برنامج يعتمد على الـ BruteForce لتخمين ارقام عضويات الفيس بوك .

متى يصبح التخمين فعال :

تكمن خطورة مثل هذه الهجمات في حالة كانت الارقام السرية سهلة وغير معقده
مثلاً مجرد ارقام / كلمة معروفة / كلمة المرور اقل من ٦ خانات .
إي ببساطة الارقام السرية التي تكون مواصفاتها بسيطة وخالية من التعقيد تقوم بتخمينها
هذة الأدوات بشكل سهل وسريع .

ماذا أفعل للحماية من التخمين :

تستخدم بعض تطبيقات الويب حماية عند ادخال اكثر من رقم سري خاطئ تتوقف امكانية الدخول
لفترة معينة أو حظر الـ Ip المهاجم ومنعه من دخول الموقع وهذه كفيلة على ما اعتقد
لأبطال مفعول هجمات الـ BruteForce .
عند اختيار كلمة مرور انتبه للمعايير التالية
١- كلمة المرور يجب ان تتكون من ١٢ خانة على الأقل .
٢- كلمة المرور يجب ان تحتوى على رموز وأحرف وأرقام .
٣- ابتعد عن كلمات المرور المعروفة مثل اسم ابنك / وألداك / مدينتك .
٤- أجعلها معقدة قدر الأمكان ولا ترمي لمعنى معين .

المؤلف : Ghost Hacker
المدونة : http://gh05th4ck.wordpress.com